REMARKS

Claims 27-33 have been examined. By this Amendment, Applicants amend independent claims 27 and 30. The amendments to these claims were previously sent to the Examiner in the form of an informal proposed amendment on August 3, 2007, in view of the interview conducted with the Examiner on July 31, 2007.

On August 17th, the Examiner called the Applicants' representative to inform them that the proposed amendment is allowable over the prior art of record, pending a new search. As such, Applicants submit that the claims are in condition for immediate allowance.

Applicants' representatives thank the Examiner for her helpful comments during the July 31st interview.

Claim Rejections – 35 U.S.C. § 102

Claims 27-33 are rejected under 35 USC 102(e) as allegedly being anticipated by U.S. Patent No. 6,088,451 to He *et al.* ("He"). For *at least* the following reasons, Applicants respectfully traverse the rejection.

Claims 27-29

Applicants respectfully submit that claim 27 is patentable over He. For example, claim 27 recites an information storage management system in a first administrative domain administered by a first organization, comprising, inter alia, a collection of stored objects, an access control unit, and a resource manager. The collection of stored objects is in the first administrative domain administered by the first organization. The access control unit is also in the first administrative domain administered by the first organization, and determines if a requestor is authorized to access a protected object stored in the collection, wherein the

collection is in the first administrative domain administered by the first organization. The resource manager is connected to the access control unit and to a communications channel. The resource manager receives a user's request for access to the protected object in the first administrative domain administered by the first organization, the request including a globally unique identifier for the user requesting the access.

In response to the user's request, the resource manager sends over the communications channel to an external storage management system in a second administrative domain a resource manager request for information about the user. The second administrative domain is administered by a second organization that is different from the first organization. The resource manager request includes the globally unique identifier. Upon receiving a response to the resource manager request from the external storage management system, the resource manager passes the user information to the access control unit in the first administrative domain administered by the first organization. The access control unit, in response to the user information, determines whether to authorize the user for access to the protected object.

The Examiner contends that network resources and information residing in various network elements 104 disclose the claimed collection of stored objects and that the local access control system (LACS) discloses the claimed access control unit (*see* He: FIG. 2, and col. 18, lines 10-11). The Examiner further contends that the user element 102 corresponds to the resource manager as set forth in claim 1. In addition, *the Examiner contends that the network security server (NSS) 208 discloses the claimed external storage management system in a second administrative domain different from the first administrative domain.* Applicants respectfully disagree.

He is directed to a system for securing access to network elements by user elements, wherein the network elements and the user elements are coupled to a network. A network security server, which is also coupled to the network, provides network security mechanisms to control access to the network elements and protect network resources and information. Each of the user elements and the network elements includes a separate local access control means as an interface that is provided at each user element and operates in conjunction with the authentication server, the credential server, and the network element access server to facilitate secure communication of data over the network (*see* He: Abstract). However, to the extent that He is directed to the protection of network elements by implementing security mechanisms, Applicants respectfully submit that the security mechanisms disclosed by He are different from the features recited in claim 27.

For instance, the following annotated version of FIG. 3 of He highlights the distinguishing features of claim 1 with respect to He.

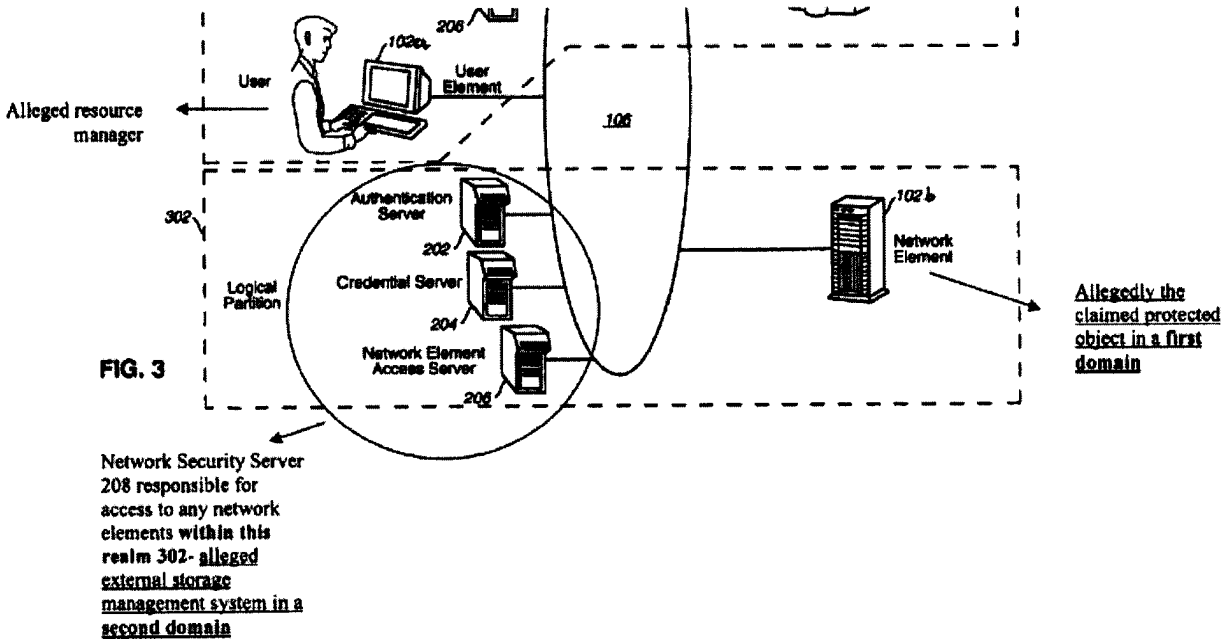

FIG. 3

In He, if the user 102a accesses a network element 102b (corresponding closest to the claimed protected object in the first administrative domain administered by the first organization) in the bottom realm 302 illustrated in FIG. 3 , the bottom realm 302 would then correspond to the claimed first administrative domain administered by the first organization. In this case, *both the network security server 208 (alleged external storage management system in a second administrative domain) and the network element 102b (alleged protected object in the first administrative domain) are part of the* ***same*** *realm administered by the same administrative entity*. Therefore, the network security server 208 in the bottom realm 302 in FIG. 3 (which includes the authentication server 202, credential server 204, and network element access server 206 in the bottom realm 302) is administered by the **same** administrative entity that also administers the requested network element 102b in the bottom realm 302 (He, col. 14, line 67 to col. 15, line 3, and col. 15, lines 8-11).

On the other hand, claim 1 recites that the resource manager receives a user's request for access to the protected object in the first administrative domain administered by the first organization, the request including a globally unique identifier for the user requesting the access, and in response to the user's request, the resource manager sends over the communications channel to an external storage management system in a second administrative domain administered by a second organization that is different from the first organization, a resource manager request for information about the user. That is, the protected object and the external storage management system are in different administrative domains, whereas in He, the network element 102b and the network security sever 208 are part of the same realm administered by the same administrative entity.

In light of the discussion above, Applicants respectfully submit that He does not disclose each and every feature of claim 27 in as complete detail as set forth in the claim. Accordingly, Applicants respectfully request the Examiner to withdraw the 35 USC 102(e) rejection of claim 27.

Since claims 28-29 depend from claim 27, Applicants respectfully submit that claims 28-29 are patentable *at least* by virtue of their dependency.

Claims 30-33

Claim 30 recites an information storage management system in a first administrative domain administered by a first organization, comprising, inter alia, a collection of stored objects, an access control unit, and a resource manager. The collection of stored objects is in the first administrative domain administered by the first organization. The access control unit is also in the first administrative domain administered by the first organization, and determines if a requestor is authorized to access a protected object stored in the collection, wherein the

collection is in the first administrative domain administered by the first organization. The resource manager is connected to the access control unit and to a communications channel. The resource manager receives a user's request for access to the protected object in the first administrative domain administered by the first organization, the request including a globally unique identifier for the user requesting the access.

In response to the user's request, the resource manager resolves the globally unique identifier to a user identifier recognized by an external storage management system in a second administrative domain. The second administrative domain is administered by a second organization that is different from the first organization. The resource manager then sends to the external storage management system a resource manager request for information about the user. The resource manager request includes the resolved user identifier. Upon receiving a response to the resource manager request from the external storage management system, the resource manager passes the user information to the access control unit in the first administrative domain administered by the first organization. The access control unit, in response to the user information, determines whether to authorize the user for access to the protected object.

Therefore, claim 30 is patentable for *at least* reasons similar to those given above with respect to claim 27. Accordingly, Applicants respectfully request the Examiner to withdraw the 35 USC 102(e) rejection of claim 30.

Since claims 31-33 depend from claim 30, Applicants respectfully submit that claims 31-33 are patentable *at least* by virtue of their dependency.

Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the

Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

Quadeer A. Ahmed
Registration No. 60,835

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON DC SUGHRUE/142133

46159
CUSTOMER NUMBER

Date: August 30, 2007